Peer to Peer (P2P) File Sharing

September 2007

ON CYBER PATROL
As covered or mandated by
0600 hours, THE PENTAGON
GOOD THING SOLDIERS NEVER VIOLATE P2P/FILE SHARING.
TEXAS HOLD 'EM
Copyright U.S. Army. All rights reserved.
1400 hours, OKLAHOMA CITY
YES, IT WOULD PUT OUR AREA PROCESSING CENTERS AT RISK.
LAND OF WARCRAFT
1600 hours, FORT HUACHUCA
JUST THINK HOW VULNERABLE THE LANDWARNET WOULD BE IF THEY DID.
THX FOR THE 75 SONGS!
2300 hours., FORT GORDON
HACKERS JUST BROKE INTO OUR SYSTEM. ANYONE KNOW HOW P2P GOT INTO THE LANDWARNET?!
NO, SIR!
NO, SIR!
NO, SIR!
A1028

Sharing Is Not “Nice” When It comes to Sensitive Data

We’ve been taught since we were kids that it’s always polite to share. That is true if it’s your cookies or toys, maybe even your lawn mower. However, sharing sensitive military information, even unknowingly, is a danger to everyone.

Peer to Peer (P2P) software such as Kazaa, Lime Wire, Morpheus and BearShare can be a treasure trove for information seekers. Many of these data miners are not merely curious surfers, but are hostile agents. There is a great deal of effort made in military, government and industry organizations to avoid this. Detailed rules and regulations, targeted training and millions of dollars of cyber-security technology are used to prevent sensitive data loss. Yet, they cannot control one key element, the actions of an individual user who loads P2P software for personal use and in doing so opens up data to the world.

The vast majority of security breaches due to P2P exposure are not intentional. In most cases, they are due to negligence or carelessness. In early summer of 2007 the House Committee on Oversight and Government Reform heard from industry and military experts about the wealth of sensitive information that was easily available via P2P applications. Some of the information that was found was the Pentagon's entire secret backbone network infrastructure diagram, data on radio frequency manipulation to beat improvised explosive devices (IED) in Iraq; physical terrorism threat assessments for three major U.S cities; and information on DoD information security system audits.

Many of the cases involved allowing family members and friends access to computers that have sensitive data on their hard drives or access to secure networks. It boils down to personal responsibility. When data leaves a secure environment is must continue to be secured. Allowing P2P applications on these computers can cause significant damage through data loss. Using P2P software yourself on such a computer is purposely ignoring a very real threat and possibly putting fellow soldiers at risk.

Classified data must be contained by using best business practices, appropriate technology and common sense. The greatest data security weakness and its greatest strength is the individual user. Regulations and rules are only valid if followed. Training is only useful if it is remembered. Physical and cyber security measures can be very effective in a closed environment, but quickly loses its power when compromised in an open environment.

Everyone with access to secure information is the ultimate lock and key that will keep inquisitive and often unfriendly information seekers out of our stored data. Share your power tools, but keep your data to yourself.